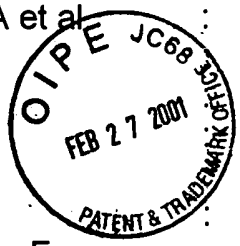
#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Takayuki SUGAHARA et al.



Serial No. 09/726,434 Art Unit: 2131

Filed: December 1, 2000 Examiner: not assigned

For: Method And Apparatus For Contents Information Atty Docket: 0102/0147

SUBMISSION OF PRIORITY DOCUMENTS

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Attached hereto please find a certified copy of applicants' Japanese application No. 2000-018437 filed in Japan on January 27, 2000.

Applicants request the benefit of said January 27, 2000 filing date for priority purposes pursuant to the provisions of 35 USC 119.

Respectfully submitted,

Louis Woo, Reg. No. 31,730
Law Offices of Louis Woo
1901 N. Fort Myer Drive, Suite 501
Arlington, Virginia 22209
Phone: (703) 522-8872

Date: Feb 27 2001

U4-0025-TH

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年　１月２７日

出 願 番 号
Application Number: 特願２０００－０１８４３７

出 願 人
Applicant (s): 日本ビクター株式会社

２０００年１２月　８日

特 許 庁 長 官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１０１６９８

【書類名】　特許願

【整理番号】　411001711

【提出日】　平成12年 1月27日

【あて先】　特許庁長官殿

【国際特許分類】　G06F　1/00

G09C　1/00

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　菅原　隆幸

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　黒岩　俊夫

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　猪羽　渉

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　上田　健二朗

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　日暮　誠司

【特許出願人】

【識別番号】　000004329

【氏名又は名称】　日本ビクター株式会社

【代表者】　守隨　武雄

【電話番号】　045-450-2423

【手数料の表示】

【予納台帳番号】　003654

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　コンテンツ情報伝送方法、コンテンツ情報記録方法、コンテンツ情報伝送装置、コンテンツ情報記録装置、伝送媒体、及び記録媒体

【特許請求の範囲】

【請求項１】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項２】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とするコンテンツ情報記録方法。

【請求項３】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項４】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の

鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

【請求項５】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報を出力する第１の鍵情報暗号化手段と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第１の鍵のもとになる情報と前記暗号化コンテンツ情報とを伝送する伝送手段と、
を設けたことを特徴とするコンテンツ情報伝送装置。

【請求項６】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報を出力する第１の鍵情報暗号化手段と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第１の鍵のもとになる情報と前記暗号化コンテンツ情報とを媒体に記録する記録手段と、
を設けたことを特徴とするコンテンツ情報記録装置。

【請求項７】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とする伝送媒体。

【請求項８】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とする記録媒体。

【請求項９】

前記ID情報は、１つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別IDに関する情報、複数人のグループを識別する識別IDに関する情報、レーティングに関する情報、機器メーカーの識別ID関する情報、コンテンツプロバイダーの識別IDに関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有IDに関する情報、接続機器の固有IDに関する情報、コンテンツの記録されたメディアの固有IDに関する情報、コンテンツを識別するIDに関する情報、課金に関する情報のうちの１つ以上の情報であることを特徴とする請求項３記載のコンテンツ情報伝送方法、または請求項４記載のコンテンツ情報記録方法、または請求項５記載のコンテンツ情報伝送装置、または請求項６記載のコンテンツ情報記録装置、または請求項７記載の伝送媒体、または請求項８記載の記録媒体。

【請求項１０】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項１１】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情

報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

【請求項１２】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とするコンテンツ情報伝送方法。

【請求項１３】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

【請求項１４】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報を出力する第１の鍵情報暗号化手段と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いて、コンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第１の鍵のもとになる情報と前記暗号化コンテンツ情報とを伝送する伝送手段と、
を設けたことを特徴とするコンテンツ情報伝送装置。

【請求項１５】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得

た暗号化第１の鍵のもとになる情報を出力する第１の鍵情報暗号化手段と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いて、コンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第１の鍵のもとになる情報と前記暗号化コンテンツ情報とを媒体に記録する記録手段と、

を設けたことを特徴とするコンテンツ情報記録装置。

【請求項１６】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とする伝送媒体。

【請求項１７】

所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とする記録媒体。

【請求項１８】

前記ID情報は、１つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別IDに関する情報、複数人のグループを識別する識別IDに関する情報、レーティングに関する情報、機器メーカーの識別ID関する情報、コンテンツプロバイダーの識別IDに関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有IDに関する情報、接続機器の固有IDに関する情報、コンテンツの記録されたメディアの固有IDに関する情報、コンテンツを識別するIDに関する情報、課金に関する情報のうちの１つ以上

の情報であることを特徴とする請求項１２記載のコンテンツ情報伝送方法、または請求項１３記載のコンテンツ情報記録方法、または請求項１４記載のコンテンツ情報伝送装置、または請求項１５記載のコンテンツ情報記録装置、または請求項１６記載の伝送媒体、または請求項１７記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンテンツ鍵とそのコンテンツ鍵を用いて暗号化された暗号化コンテンツ情報を伝送、記録するためのコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体に関するものである。そして、この発明は、特にコンテンツ情報を正規の制限下においてのみ的確に再生（復号）させることを可能とするコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体を提供することを目的としている。

【０００２】

【従来の技術】

暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのディジタルデータを配信する有用な方法として、特開平１０－２６９２８９のディジタルコンテンツ配布管理方法、ディジタルコンテンツ再生方法及び装置がある。この発明では、ディジタルコンテンツの配布側では、ディジタルコンテンツを暗号化及び圧縮して加工し、この加工したディジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信する。そして、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしている。一方、ディジタルコンテンツの再生側では、その加工されたディジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツ使用情報を配布側に送信するようにし、記録されたコンテンツを持ち運びできるようにした。

【０００３】

また、特開平１０－２８３２６８の情報記記録媒体、記録装置、情報伝送シス

テム、暗号解読装置では、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるものにおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が追加記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザ側で暗号化された情報をそのままＨＤＤや光ディスクにコピーして不正使用をすることを防止しするようにしている。

【０００４】

【発明が解決しようとする課題】

しかし、上記従来の方式では、暗号化コンテンツ情報の再生（復号）に制限を加えて、正規の条件下以外の不正な再生（復号）を防止するようにしているが、その制限情報は第三者により容易に変更することが可能であり、不正な条件下での再生（復号）を的確に防止することが難しかった。

この発明は、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とするコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体を提供することを目的としている。

【０００５】

【課題を解決するための手段】

そこで、上記課題を解決するために本発明は、下記の各方法・装置を提供するものである。

（１）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とするコンテンツ情報伝送方法。

（２）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の

鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

（３）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を伝送することを特徴とするコンテンツ情報伝送方法。

（４）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、
を記録することを特徴とするコンテンツ情報記録方法。

（５）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報を出力する第１の鍵情報暗号化手段と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第１の鍵のもとになる情報と前記暗号化コンテンツ情報とを伝送する伝送手段と、
を設けたことを特徴とするコンテンツ情報伝送装置。

（６）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報を出力する第１の鍵情報暗号化手段と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の

鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第１の鍵のもとになる情報と前記暗号化コンテンツ情報とを媒体に記録する記録手段と、

を設けたことを特徴とするコンテンツ情報記録装置。

（７）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とする伝送媒体。

（８）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とする記録媒体。

（９）　前記ID情報は、１つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別IDに関する情報、複数人のグループを識別する識別IDに関する情報、レーティングに関する情報、機器メーカーの識別ID関する情報、コンテンツプロバイダーの識別IDに関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有IDに関する情報、接続機器の固有IDに関する情報、コンテンツの記録されたメディアの固有IDに関する情報、コンテンツを識別するIDに関する情報、課金に関する情報のうちの１つ以上の情報であることを特徴とする上記（３）記載のコンテンツ情報伝送方法、または上記（４）記載のコンテンツ情報記録方法、または上記（５）記載のコンテンツ情報伝送装置、または上記（６）記載のコンテンツ情報記録装置、または上記（７）記載の伝送媒体、または上記（８）記載の記録媒体。

（１０）　所定の縮退関数により特定の認証子値が得られるように設定されたID

情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とするコンテンツ情報伝送方法。

（１１）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とするコンテンツ情報記録方法。

（１２）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とするコンテンツ情報伝送方法。

（１３）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とするコンテンツ情報記録方法。

（１４）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報を出力する第１の鍵情報暗号化手段と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いて、コンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第１の鍵のもとになる情報と前記暗号化コンテンツ情報とを伝送す

る伝送手段と、

を設けたことを特徴とするコンテンツ情報伝送装置。

（１５）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報を出力する第１の鍵情報暗号化手段と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いて、コンテンツ情報を暗号化した暗号化コンテンツ情報を出力するコンテンツ情報暗号化手段と、

前記暗号化第１の鍵のもとになる情報と前記暗号化コンテンツ情報とを媒体に記録する記録手段と、

を設けたことを特徴とするコンテンツ情報記録装置。

（１６）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を伝送することを特徴とする伝送媒体。

（１７）　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報に対し、少なくとも前記ID情報部分を暗号化して得た暗号化第１の鍵のもとになる情報と、

前記第１の鍵のもとになる情報から生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報と、

を記録することを特徴とする記録媒体。

（１８）　前記ID情報は、１つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別IDに関する情報、複数人のグループを識別する識別IDに関する情報、レーティングに関する情報、機器メーカーの識別ID関する情報、コンテンツプロバイダーの識別IDに関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有IDに関する情報

、接続機器の固有IDに関する情報、コンテンツの記録されたメディアの固有IDに関する情報、コンテンツを識別するIDに関する情報、課金に関する情報のうちの１つ以上の情報であることを特徴とする上記（１２）記載のコンテンツ情報伝送方法、または上記（１３）記載のコンテンツ情報記録方法、または上記（１４）記載のコンテンツ情報伝送装置、または上記（１５）記載のコンテンツ情報記録装置、または上記（１６）記載の伝送媒体、または上記（１７）記載の記録媒体。

【０００６】

【発明の実施の形態】

図１に本発明のコンテンツ情報記録装置またはコンテンツ情報伝送装置の第１実施例の概略構成を示す。なお、本説明においては、磁気記録媒体、光記録媒体、半導体メモリ等を記録媒体と呼び、光ケーブル、電線、無線伝送路等の信号を伝送する伝送媒体を伝送路と呼ぶこととする。

【０００７】

まず、記録側または送信側（伝送側）の説明をする。図１に示すように、一方向性関数演算装置１は、第１の鍵のもとになる情報から一方向性の関数を用いて原始鍵を作成する。第１の鍵のもとになる情報は、例えば図３に示すように、１６ビットのコンテンツプロバイダーIDと、同じく１６ビットのコンテンツオーサーIDと、４ビットのメーカーIDと、システム固有の２０ビットの情報の計５６ビットで構成する。

【０００８】

一方向性関数とは、一方向性ハッシュ関数とも表現でき、関数hとその定義域のある値xが与えられてh(x) = h(y)となるようなyを求めることが困難な関数のことである。コンテンツはMPEGなどの所定の圧縮方式によって圧縮された後、DESなどの暗号化を用いる。DES暗号化方式は１９７７年にアメリカ連邦政府標準に採用されたもので代表的な共通鍵暗号化方式で５６ビットの鍵を用いて６４ビット単位で暗号化復号化を行うブロック暗号化方式である。暗号化は６４ビットの平分を３２ビットづつに分割して転置、置換、非線型関数、排他的論理和により構成されている。例えばDESの場合、暗号化鍵は５６ビット程度である。従って

、一方向性関数の出力ビット数が５６ビットになるような第１の鍵のもとになる情報は、例えば図３のように全体の長さを５６ビットの情報としておく。

【０００９】

一方向性関数演算装置１で生成された原始鍵は、コンテンツ鍵生成器２に入力される。また、コンテンツ鍵生成器２には、予め設定された所定の認証子値が、メモリーもしくはCPU等を備えた認証値子発生器３から入力される。

【００１０】

なお、所定の認証子値（特定の認証子値）が、後述する再生側の所定の縮退関数により得られるように、縮退関数のパラメータとなる前記ID情報（第１の鍵のもとになる情報に含まれる前記ID情報：図３に示す例ではコンテンツプロバイダーIDと、同じく１６ビットのコンテンツオーサーIDと、４ビットのメーカーID）の値を設定しておく。このID情報は正規の使用者にのみ公開されるものであり、許可されたID情報とも呼べるものである。

【００１１】

コンテンツ鍵生成器２は、入力された原始鍵の情報と認証子の情報を用いて、所定の関数により第１の鍵（コンテンツ鍵）を生成する。例えば、図４に示すように、原始鍵情報と認証子情報との排他的論理和を計算することで第１の鍵（コンテンツ鍵）を生成する。

【００１２】

生成された第１の鍵を用いて、コンテンツ情報をコンテンツ情報暗号化装置４により暗号化する。そして、暗号化コンテンツ情報を記録または伝送する。暗号化にはDESなどの暗号化方式を用いる。

【００１３】

記録媒体に記録、もしくは伝送媒体により伝送される情報は、暗号化されたコンテンツ情報（暗号化コンテンツ情報）と、第１の鍵のもとになる情報である。なお、第１の鍵のもとになる情報を、少なくとも前記ID情報部分を暗号化して暗号化された第１の鍵のもとになる情報（暗号化第１の鍵のもとになる情報）として記録または伝送するようにしてもよい。

【００１４】

次に、再生側または受信側の説明をする。記録媒体から再生された、もしくは伝送媒体により伝送されてきた第１の鍵のもとになる情報から、一方向性関数演算装置５により一方向性関数を用いて原始鍵を生成する。暗号化された第１の鍵のもとになる情報が供給された場合は、その情報を復号化して第１の鍵のもとになる情報を得てから原始鍵を生成する。

【００１５】

また、第１の鍵のもとになる情報に含まれている前記ID情報を用いて、縮退関数演算装置６により前記した認証子値を生成する。縮退関数演算装置６に用いる縮退関数は、一方向性関数演算装置５に用いる一方向性関数とは別の関数としてもよい。

【００１６】

縮退関数は、例えば図６に示すように、ID情報である１６ビットのコンテンツプロバイダーIDと、同じく１６ビットのコンテンツオーサーIDと、４ビットのメーカーIDとの情報の排他的論理和を求めるような関数でもよい。

【００１７】

一方向性関数演算装置５により生成された原始鍵の情報と、縮退関数演算装置６により生成された認証子値の情報とは、コンテンツ鍵生成器７に入力され、所定の関数により第１の鍵（コンテンツ鍵）が生成される。所定の関数は、例えば図５に示す原始鍵の情報と、認証子値の情報との２つの情報に対して排他的論理和を計算するような関数でよい。

【００１８】

この生成された第１の鍵（コンテンツ鍵）を用いて、記録媒体から再生された、もしくは伝送媒体により伝送された暗号化コンテンツ情報をコンテンツ情報復号化装置８で復号化する。これによってコンテンツ情報を再生することが可能となる。

【００１９】

前述したように、所定の認証子値（特定の認証子値）が所定の縮退関数により得られるように、第１の鍵のもとになる情報に含まれるID情報の値が設定されている。このID情報は正規の使用者にのみ公開されるものである。従って、不正な

使用者が適当な値のID情報により暗号化コンテンツ情報を復号化しようとしても、特定の認証子値が得られないので復号化できない。また、所定の縮退関数の情報も正規の使用者にのみ公開されるものであるので、たとえID情報の値が漏洩したとしても、その情報から直ちに正規の特定の認証子値がえられものではない。このように上記実施例は、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とするものである。

【００２０】

次に、第２実施例について図２と共に説明する。この実施例は、コンテンツ情報の暗号化側において、認証子値を第１の鍵（コンテンツ鍵）生成に反映しないものである。図２において図１と同一の部分には同一の符号を付す。

【００２１】

まず、記録側または送信側（伝送側）の説明をする。図２に示すように、一方向性関数演算装置１は、第１の鍵のもとになる情報から一方向性の関数を用いて原始鍵を作成する。第１の鍵のもとになる情報は、例えば図３に示すように、１６ビットのコンテンツプロバイダーIDと、同じく１６ビットのコンテンツオーサーIDと、４ビットのメーカーIDと、システム固有の２０ビットの情報の計５６ビットで構成する。

【００２２】

一方向性関数演算装置１で生成された原始鍵はそのまま第１の鍵（コンテンツ鍵）となり、この第１の鍵を用いて、コンテンツ情報をコンテンツ情報暗号化装置４により暗号化する。そして、暗号化コンテンツ情報を記録または伝送する。暗号化にはDESなどの暗号化方式を用いる。

【００２３】

なお、第１の鍵のもとになる情報に含まれる前記ID情報（コンテンツプロバイダーIDと、同じく１６ビットのコンテンツオーサーIDと、４ビットのメーカーID）は、第１実施例と同様に再生側で所定の縮退関数のパラメータとなるものであり、ID情報の値は、予め設定された所定の認証子値（特定の認証子値）が、所定の縮退関数により得られるように設定されたものである。このID情報は、当然正

規の使用者にのみ公開されるものである。

【００２４】

記録媒体に記録もしくは伝送媒体により伝送される情報は、暗号化されたコンテンツ情報（暗号化コンテンツ情報）と、第１の鍵のもとになる情報である。なお、第１の鍵のもとになる情報を、少なくとも前記ID情報部分を暗号化して暗号化された第１の鍵のもとになる情報（暗号化第１の鍵のもとになる情報）として記録または伝送するようにしてもよい。

【００２５】

次に、再生側または受信側の説明をする。記録媒体から再生された、もしくは伝送媒体により伝送されてきた第１の鍵のもとになる情報から、一方向性関数演算装置５により一方向性関数を用いて原始鍵を生成する。この原始鍵がそのまま第１の鍵（コンテンツ鍵）となる。暗号化された第１の鍵のもとになる情報が供給された場合は、その情報を復号化して第１の鍵のもとになる情報を得てから原始鍵を生成する。

【００２６】

また、第１の鍵のもとになる情報に含まれている前記ID情報を用いて、縮退関数演算装置６により前記した認証子値を生成する。縮退関数演算装置６に用いる縮退関数は、一方向性関数演算装置５に用いる一方向性関数とは別の関数としてもよい。

【００２７】

縮退関数は、例えば図６に示すように、１６ビットのコンテンツプロバイダーIDと、同じく１６ビットのコンテンツオーサーIDと、４ビットのメーカーIDとの情報の排他的論理和を求めるような関数でもよい。

【００２８】

一方向性関数演算装置５により生成された原始鍵、即ち第１の鍵（コンテンツ鍵）の情報と、縮退関数演算装置６により生成された認証子値の情報とは、コンテンツ鍵加工器１１に入力される。コンテンツ鍵加工器１１は前記予め設定されている特定の認証値子の情報が供給された場合のみ、入力される第１の鍵（コンテンツ鍵）の情報をそのまま出力するものであり、特定の認証値子以外の情報が

供給された場合には、入力される第１の鍵情報を加工して（値を変更して）出力する。

【００２９】

コンテンツ鍵加工器１１から出力された第１の鍵（コンテンツ鍵）を用いて、記録媒体から再生された、もしくは伝送媒体により伝送された暗号化コンテンツ情報をコンテンツ情報復号化装置８で復号化する。正規の特定の認証値子がコンテンツ鍵加工器１１に供給されれば、正しい第１の鍵（コンテンツ鍵）がコンテンツ情報復号化装置８に入力され、これによってコンテンツ情報を再生することが可能となる。

【００３０】

このように本実施例によれば、正規の特定の認証値子が得られないければ暗号化コンテンツ情報を復号化できず、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とするものである。

【００３１】

次に、第３実施例について図７と共に説明する。本実施例において、コンテンツ情報の暗号化側（記録側または送信側）は図２に示す第２実施例と同様であるので、ここでは、再生側または受信側について説明する。

【００３２】

記録媒体から再生された、もしくは伝送媒体により伝送されてきた第１の鍵のもとになる情報から、一方向性関数演算装置５により一方向性関数を用いて原始鍵を生成する。この原始鍵がそのまま第１の鍵（コンテンツ鍵）となる。暗号化された第１の鍵のもとになる情報が供給された場合は、その情報を復号化して第１の鍵のもとになる情報を得てから原始鍵を生成する。

【００３３】

また、第１の鍵のもとになる情報に含まれている前記ID情報を用いて、縮退関数演算装置６によって認証子値を生成する。縮退関数演算装置６に用いる縮退関数は、一方向性関数演算装置５に用いる一方向性関数とは別の関数としてもよい。

【００３４】

縮退関数は、例えば図６に示すように、１６ビットのコンテンツプロバイダーIDと、同じく１６ビットのコンテンツオーサーIDと、４ビットのメーカーIDとの情報の排他的論理和を求めるような関数でもよい。

【００３５】

縮退関数演算装置６により生成された認証子値は、認証子値正当性判定器１２に供給され、正規の特定の認証値子であるか否かが判定される。認証子値正当性判定器１２の判定結果はコンテンツ情報復号化装置８ａに供給され、コンテンツ情報復号化装置８ａは、判定結果が「正規の特定の認証値子」である場合のみ復号動作を行う。

【００３６】

上記判定結果が「正規の特定の認証値子」である場合には、コンテンツ情報復号化装置８ａは、一方向性関数演算装置５により生成された第１の鍵（コンテンツ鍵）を用いて、記録媒体から再生された、もしくは伝送媒体により伝送された暗号化コンテンツ情報を復号化する。これによってコンテンツ情報を再生することが可能となる。

【００３７】

このように本実施例によれば、正規の特定の認証値子が得られないければ暗号化コンテンツ情報を復号化できず、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とするものである。

【００３８】

なお、第１の鍵のもとになる情報に含まれる前記ID情報としは、１つ以上の国、地域、空間を定義したリージョンに関する情報、個人の識別IDに関する情報、複数人のグループを識別する識別IDに関する情報、レーティングに関する情報、機器メーカーの識別ID関する情報、コンテンツプロバイダーの識別IDに関する情報、時間に関する情報、コンテンツオーサリング者に関する情報、コンテンツを再生する再生機器の固有IDに関する情報、接続機器の固有IDに関する情報、コンテンツの記録されたメディアの固有IDに関する情報、コンテンツを識別するIDに

関する情報、課金に関する情報のうちの１つ以上の情報を用いることが考えられる。

【００３９】

【発明の効果】

以上の通り、本発明によれば、正規のID情報にもとづく正規の特定の認証値子が得られないければ暗号化コンテンツ情報を復号化できないので、不正な条件下でのコンテンツ情報の再生（復号）をより確実に防止し、正規の条件下での再生（復号）を的確に行うことを可能とする。

【図面の簡単な説明】

【図１】

第１実施例の概略構成を示す図である。

【図２】

第２実施例の概略構成を示す図である。

【図３】

第１の鍵のもとになる情報の構成例を示す図である。

【図４】

図１に示す暗号化側のコンテンツ鍵生成器の説明図である。

【図５】

図１に示す復号化側のコンテンツ鍵生成器の説明図である。

【図６】

復号化側の縮退関数の例を示す図である。

【図７】

第３実施例の概略構成を示す図である。

【符号の説明】

１，５　一方向性関数演算装置

２，７　コンテンツ鍵生成器

３　認証子値発生器

４　暗号化装置

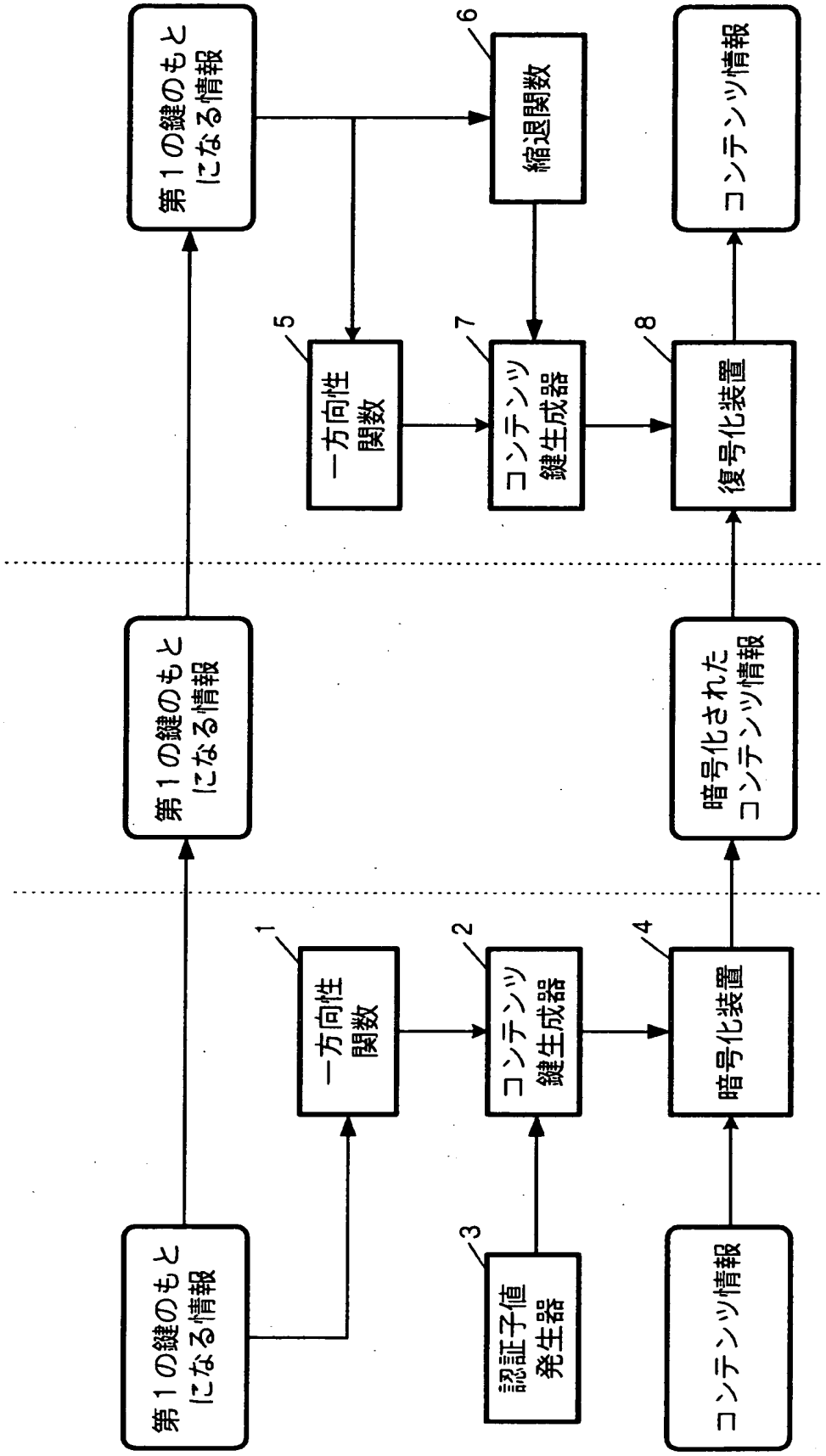
６　縮退関数演算装置

８　コンテンツ情報復号化装置

【書類名】　　図面

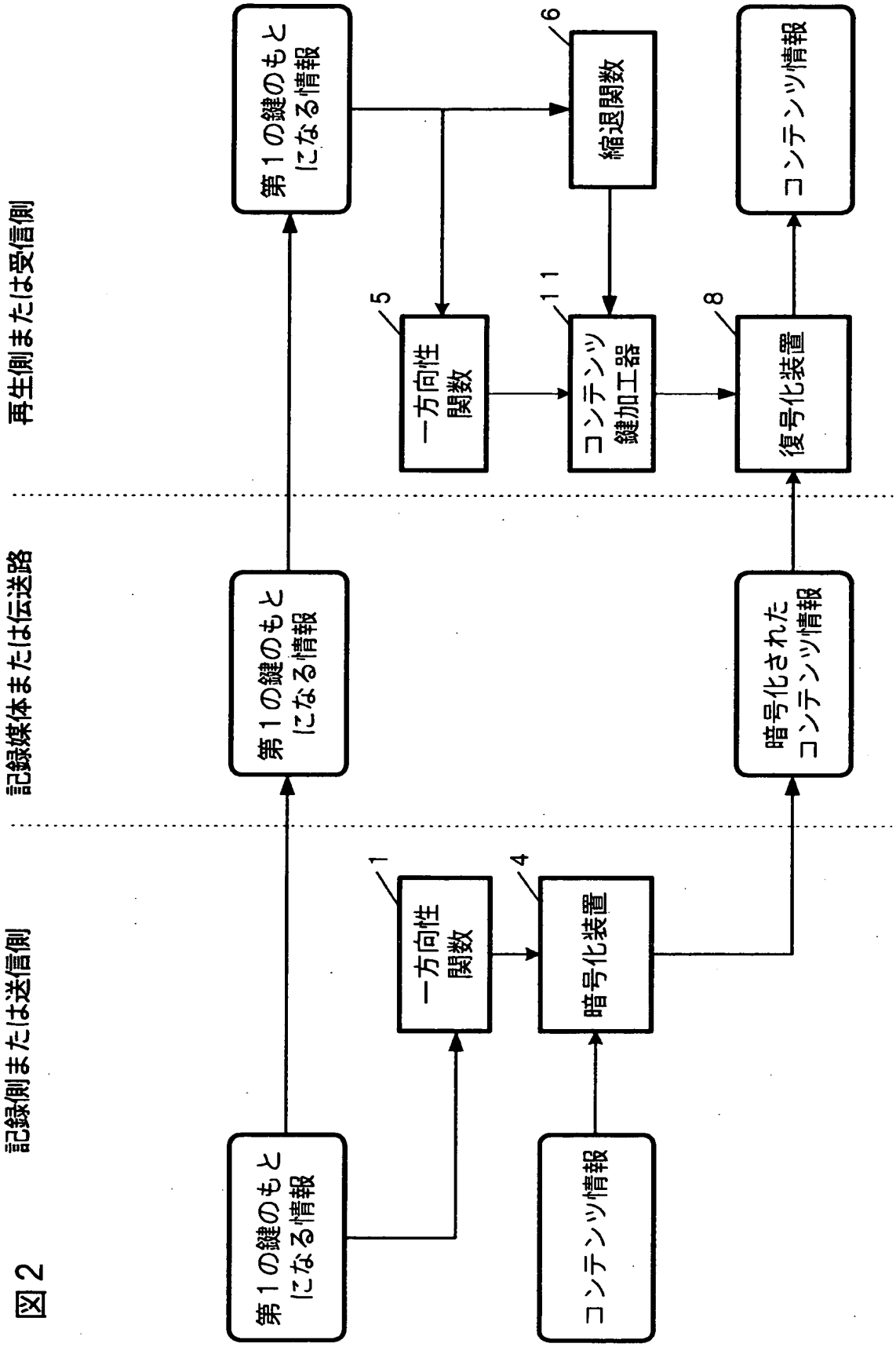
【図１】

図１


記録側または送信側
記録媒体または伝送路
再生側または受信側
第１の鍵のもとになる情報
一方向性関数
1
コンテンツ鍵生成器
2
認証子値発生器
3
暗号化装置
4
コンテンツ情報
第１の鍵のもとになる情報
一方向性関数
5
縮退関数
6
コンテンツ鍵生成器
7
復号化装置
8
暗号化されたコンテンツ情報
コンテンツ情報

【図２】

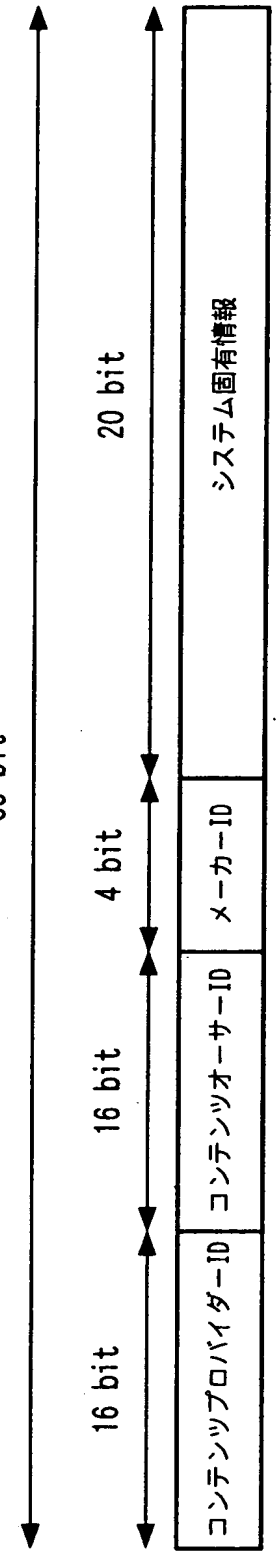
図２


記録側または送信側
記録媒体または伝送路
再生側または受信側
第１の鍵のもとになる情報
一方向性関数
1
暗号化装置
4
コンテンツ情報
第１の鍵のもとになる情報
縮退関数
6
一方向性関数
5
コンテンツ鍵加工器
11
復号化装置
8
コンテンツ情報
第１の鍵のもとになる情報
暗号化されたコンテンツ情報

【図３】

図３

第１の鍵のもとになる情報



【図４】

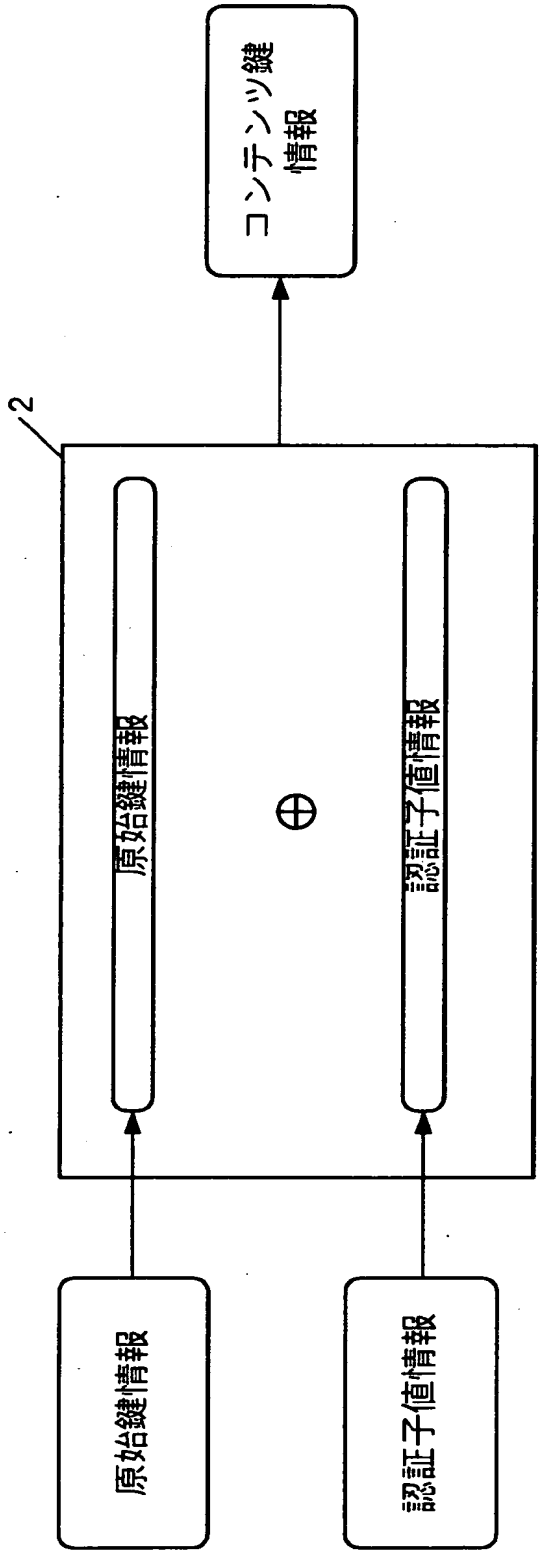


図４

【図５】

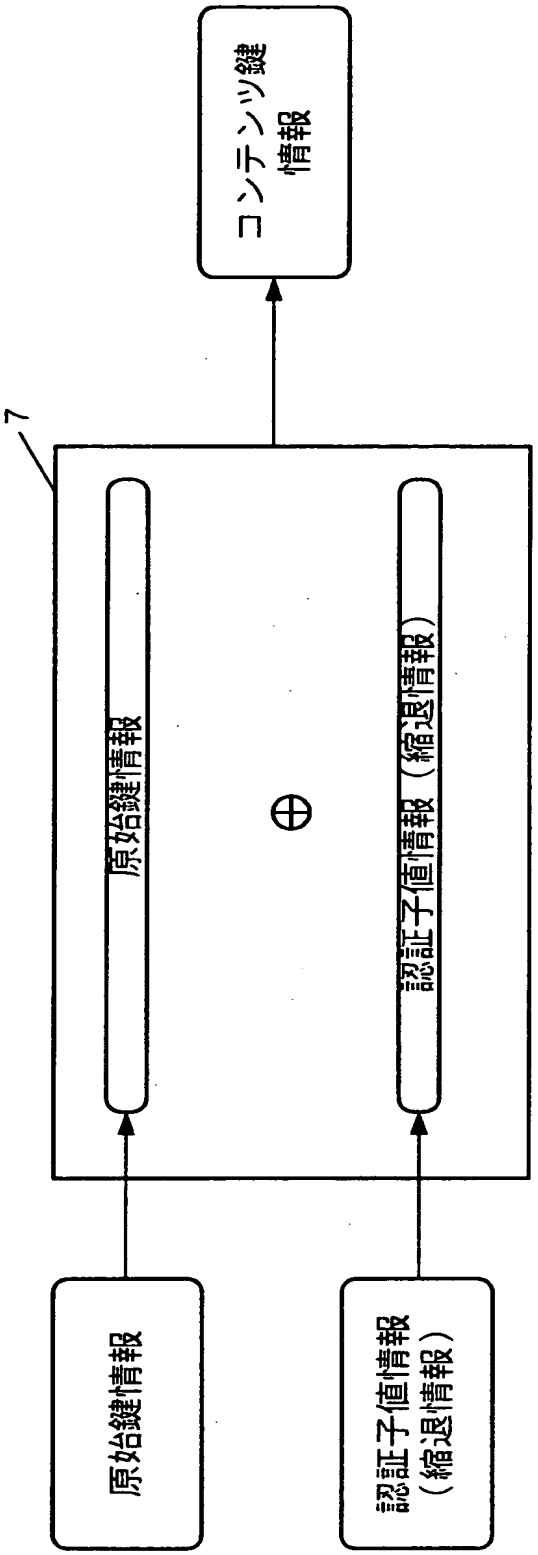


図５

【図６】

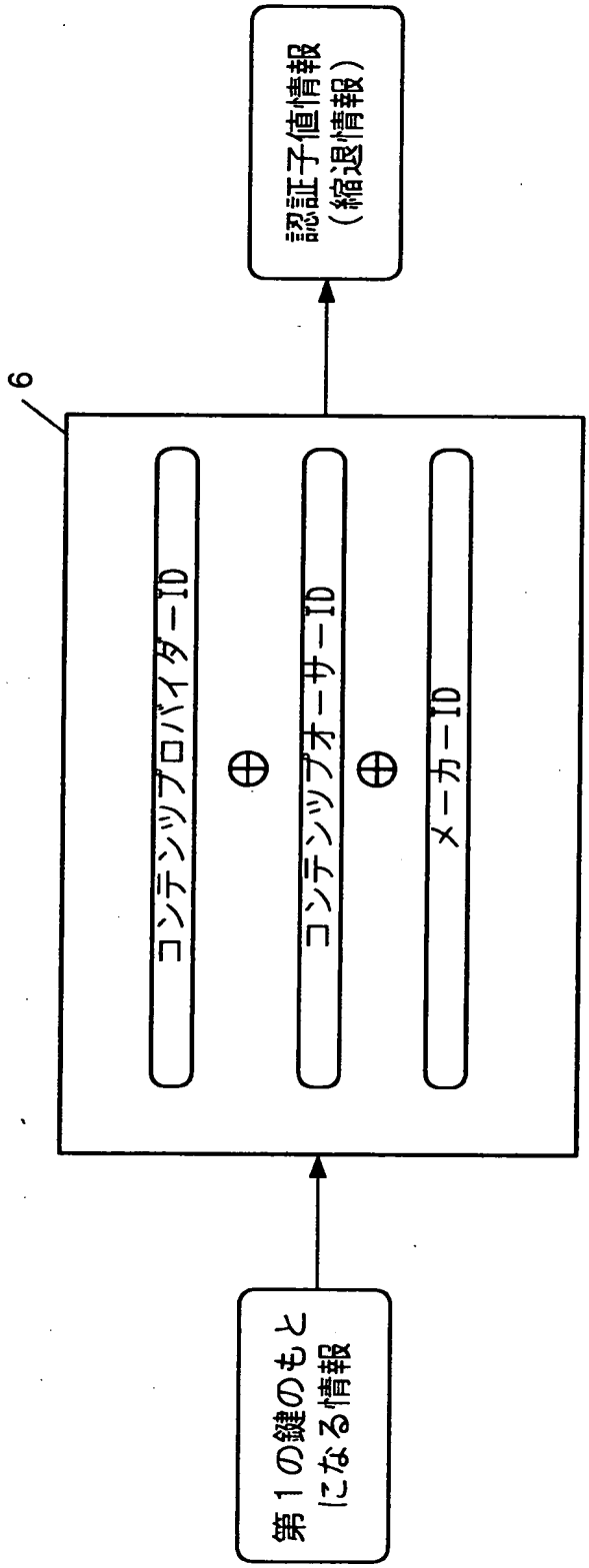

認証子値情報
（縮退情報）
6
コンテンツプロバイダーID
⊕
コンテンツオーサーID
⊕
メーカーID
第１の鍵のもと
になる情報

図６

【図７】

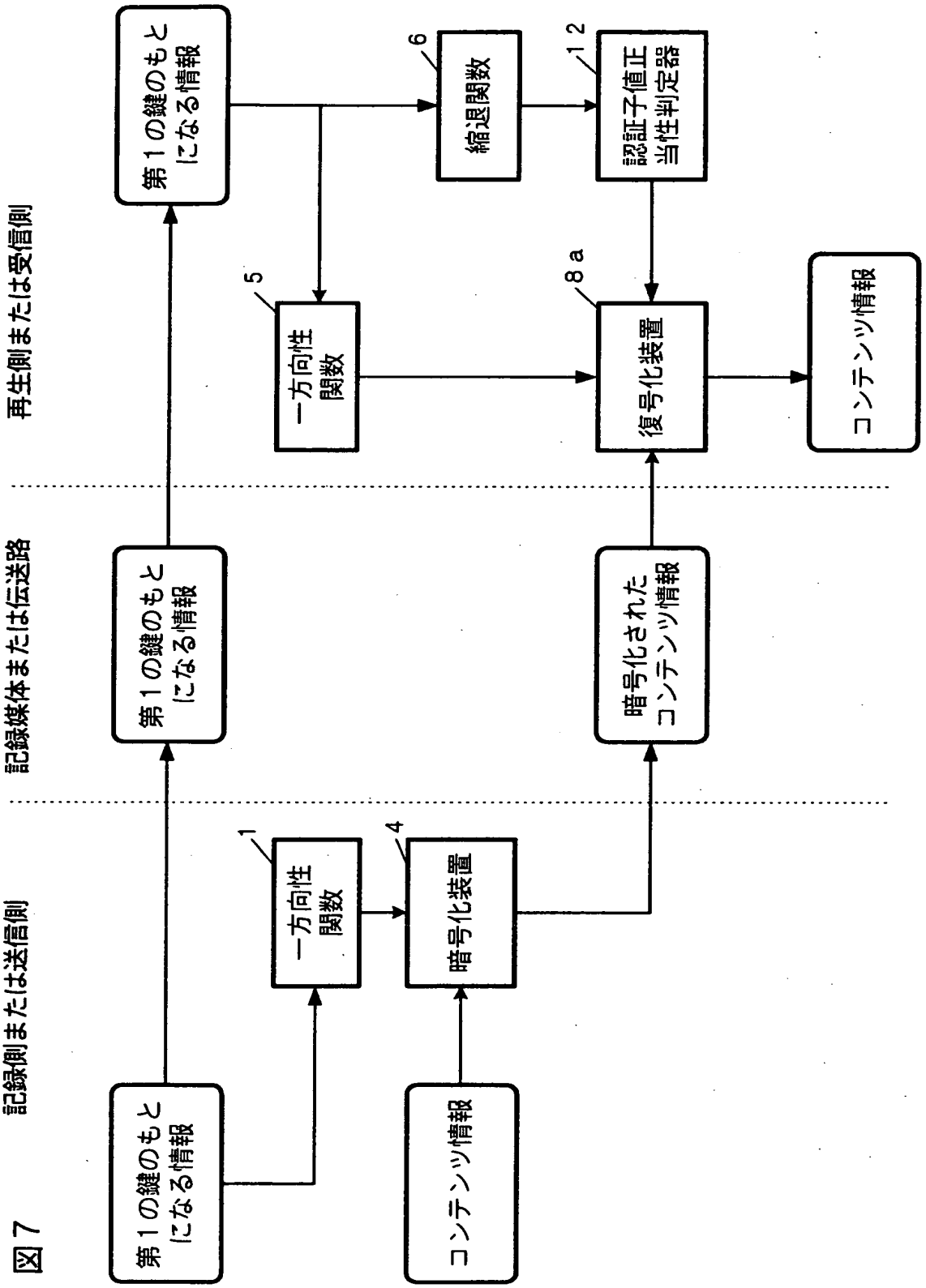

再生側または受信側
記録媒体または伝送路
記録側または送信側
第１の鍵のもとになる情報
縮退関数
6
認証子値正当性判定器
12
一方向性関数
5
復号化装置
8a
コンテンツ情報
第１の鍵のもとになる情報
暗号化されたコンテンツ情報
一方向性関数
1
暗号化装置
4
第１の鍵のもとになる情報
コンテンツ情報

図７

【書類名】　　要約書

【要約】

【課題】　暗号化コンテンツ情報を正規の制限下においてのみ的確に再生（復号）させることを可能とするコンテンツ情報伝送方法、記録方法、伝送装置、記録装置、伝送媒体、及び記録媒体を提供すること。

【解決手段】　所定の縮退関数により特定の認証子値が得られるように設定されたID情報を含む第１の鍵のもとになる情報と、前記第１の鍵のもとになる情報と前記特定の認証子値とから生成された第１の鍵を用いてコンテンツ情報を暗号化した暗号化コンテンツ情報とを伝送または記録する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４３２９〕

１．変更年月日　　１９９０年　８月　８日
　［変更理由］　新規登録
　　住　所　　神奈川県横浜市神奈川区守屋町３丁目１２番地
　　氏　名　　日本ビクター株式会社